UNITED STATES DISTRICT COURT
DISTRICT OF ALASKA

UNITED STATES OF AMERICA, Plaintiff, vs. LUKE EDWARD FOSTER, Defendant.	3:21-CR-000114-SLG-MMS **FINAL REPORT AND RECOMMENDATION ON MOTION TO SUPPRESS [DKT. 36]**

I. MOTION PRESENTED

The indictment, filed in December 2021, charges Luke Edward Foster with one count of distribution of controlled substances,[1] one count of possession of controlled substances with intent to distribute,[2] and one count of possession of firearms in furtherance of a drug-trafficking crime.[3] Foster moves to suppress all the evidence following a June 2021 search warrant on several bases: (1) a tower dump is a search under the Fourth Amendment; (2) tower dumps should be subject to constitutional safeguards; (3) the search warrant was an unlawful search "of historical cell site location information (CSLI) of all individuals whose phones connected to several cell-phone towers during designated periods"; because the search warrant was (4) stale; (5) lacked particularity; (6) the evidence

[1] 21 U.S.C. § 841(a)(1), (b)(1)(C)
[2] 21 U.S.C. § 841(a)(1), (b)(1)(C)
[3] 18 U.S.C. § 924(c)(1)(A)(i)

following the tower dump is fruit of the poisonous tree; and (7) *Leon*'s good-faith exception does not apply. *See generally* Dkt. 36.

The government responds that (1) a warrant was not required for the tower dump because there was no search under the Fourth Amendment; (2) the search warrant established probable cause; (3) the search warrant "described a narrow and specific group of records"; (4) Foster's constitutional rights were safeguarded; (5) Foster lacks standing to challenge law enforcement activity on behalf of others; and (6) the *Leon* good-faith exception would nonetheless apply. *See generally* Dkt. 42.

This Court, in September 2022, denied Foster's request for an evidentiary hearing, and instead held oral argument. Dkt. 44; Dkt. 45. The facts are drawn from law enforcement reports, from the search warrant, and from the parties' briefs. Dkt. 36; Dkt. 36-1 to 36-4; Dkt. 42.

This Court hereby issues its Final Report and Recommendation regarding Foster's Motion to Suppress. Dkt. 36. For the reasons below, Foster's Motion to Suppress should be **DENIED**. 28 U.S.C. § 636(b)(1)(B).

II. FACTUAL HISTORY

A. Swastika Stickers

A lasting symbol of the Nazi regime has been the swastika. As the Ninth Circuit has noted, "[r]egardless of its ancient or historic origins, the swastika today is a potent symbol of intolerance, hatred, and violence." *Dickinson v. Austin*, 942 F.2d 791 (9th Cir. 1991); *see also* https://www.adl.org/resources/hate-symbol/swastika ("Since 1945, the swastika has served as the most significant and notorious of hate symbols, anti-Semitism, and white

supremacy … In the United States, the swastika is overwhelmingly viewed as a hate symbol.").

Perhaps motivated by the anniversary of George Floyd's murder, an individual, now identified as Foster, placed swastika stickers at different locations around Anchorage in the early morning hours of May 25, 2021. Dkt. 36-2 at 12-18; Dkt. 42 at 4.

The first location was the Alaska Jewish Museum. Dkt. 36-1 at 1-2; Dkt. 36-2 at 12-14. A review of the museum's video cameras showed that around 2:00 a.m., a "Toyota RAV4 [drove] erratically" through the parking lot before Foster mounted a one-wheeled scooter to place three to four swastika stickers around the museum. *Id.*; *Id.* The video camera showed Foster wearing sandals and dark-colored clothing. Dkt. 36-2 at 11-12. Foster, at one point, "raise[d] a middle finger to the surveillance camera. The surveillance footage" showed Foster "using a cell phone to possibly take photographs of some of the stickers after they were placed and to send what appear to be text messages." Dkt. 36-1 at 2; Dkt. 36-2 at 12-13. The Alaskan Jewish community felt "threatened" and in fear for their lives. *Id.* at 14-15.

The second location was the Planned Parenthood Clinic. Dkt. 36-1 at 6; Dkt. 36-2 at 15. From 2:21 a.m. to 2:26 a.m., Foster was recorded on surveillance video, alleged to be driving the same RAV4 and in the same clothing, "appear[ing] to be aware of the locations of surveillance cameras and made gestures towards them several times." *Id.*; *Id.*

The third location was the University of Alaska. *Id.* at 8; *Id.* at 17. Although video cameras did not capture Foster's every movement, it appears that Foster placed about six stickers from 2:29 a.m. to 2:35 a.m. *Id.*; *Id.*

The fourth location was a bank, with traffic cameras recording Foster, or someone similar to Foster, placing stickers around the bank. *Id.*; *Id.*

The fifth location was a LGBTQ+ friendly bar. *Id.* at 2-3; *Id.* at 16. In the same clothing and on the same one-wheeled scooter, Foster placed about four swastika stickers around 2:47 a.m. *Id.*; *Id.* It is alleged that Foster "executed a Nazi-style salute, raised a middle finger to the security camera, and rode away." *Id.*; *Id.* The bar's manager believed that the stickers were explicit threats of intimidation because Nazis have historically persecuted LGBTQ+ members. *Id.*; *Id.* at 16-17. A local politician also phoned the Federal Bureau of Investigation to report the stickers as "a potential hate incident." Dkt. 36-1 at 2.

The sixth location was at an intersection at Old Seward Highway and Dimond Boulevard. Dkt. 36-1 at 5; Dkt. 36-2 at 17. There was no video recording of the sticker placement. *Id.*; *Id.*

On May 27, the FBI opened an investigation to inquire into whether federal hate crimes had been violated, as there was "an articulable factual basis that an unknown male subject defaced religious property because of the ethnic characteristics of individuals associated with that religious property and obstructed by threat of force [*sic*] individuals' enjoyment of religious beliefs. Dkt. 36-1 at 1-3 (internal quotations omitted).

The last location occurred that same day, May 27. Dkt. 36-2 at 18. It was alleged that a swastika sticker was placed on a vehicle while the vehicle's owner was at a local park. *Id.* After noticing the sticker, and aware of the previous sticker incidents, the vehicle's owner notified law enforcement. *Id.*

B. Tower Dump Search Warrant

In June 2021, FBI Special Agent Kirk Oberlander applied for three 18 U.S.C. § 2703(c)(1)(A) warrants for "[r]ecords and information associated with communications to and from cellular antenna towers ("cell towers") that service the identified addresses on the identified dates and timeframes [*sic*] that are within the possession, custody, or control of [telephone companies]." Dkt. 36-2 at 3; Dkt. 36-3 at 3; Dkt. 36-4 at 3.[4] SA Oberlander believed there was probable cause that several statutes had been violated: 18 U.S.C. §§ 245, 247, and 248. Dkt. 36-2 at 9. Otherwise known as "tower dumps," such warrants are a "download of information on all the devices that connected to a particular cell site during a particular interval." *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018). The tower dump information here consisted of: (1) a cell phone number and unique identifiers for each cell phone that were within the area of the cell tower; (2) the sector of the relevant tower that catalogued a radio signal from "the locally served wireless device"; and (3) "the date, time, and duration of each communication." Dkt. 36-2 at 4-5, 9-10; Dkt. 42 at 3-4; *see also Carpenter*, 138 S. Ct. at 2211-2212 (describing cell site data). SA Oberlander's application, in other words, sought identifying information for all phones within the geographical ambit of eight cell towers, near the seven vandalized locations, for limited identified hours on May 25 and May 27:

Service Location	Date	Time frame
Alaska Jewish Museum	May 25, 2021	1:50 a.m. - 2:10 a.m.
Planned Parenthood	May 25, 2021	2:10 a.m. - 2:30 a.m.

[4] Dkt. 36-2 is a warrant for GCI, Dkt. 36-3 is a warrant for AT&T, and Dkt. 36-4 is a warrant for Verizon. The warrants are otherwise identical and will be cited under one *Id.* for efficiency purposes.

University of Alaska	May 25, 2021	2:20 a.m. - 2:45 a.m.
University of Alaska	May 25, 2021	2:20 a.m. - 2:35 a.m.
Bank	May 25, 2021	2:26 a.m. - 2:46 a.m.
LGBTQ+ Bar	May 25, 2021	2:36 a.m. - 2:57 a.m.
Old Seward Hwy. and Dimond Blvd. Intersection	May 25, 2021	1:15 a.m. - 3:45 a.m.
Local Park	May 27, 2021	10:00 p.m. - 11:30 p.m.

Id. at 3.

After describing his qualifications and law enforcement experience, SA Oberlander stated that he generally understood that cell phones are used for criminal activity, including logistics, and that cell phones are generally used while a crime is being committed. *Id.* at 7-9. This was relevant for probable cause purposes because "the surveillance video depict[ed] [Foster] using a cellular telephone at the Anchorage Jewish Museum." *Id.* at 19. SA Oberlander attested that the tower dump information had a minimized scope, was limited in time frames, and the commercial nature of the locations would also lessen the amount of third-party data collection. *Id.* at 19-20.

This Court, in June 2021, granted the three warrants. Dkt. 36-2 to 36-4.

C. Further Investigation into Foster

Using information derived from these three warrants, law enforcement identified Foster as a potential suspect because Foster's cell phone, registered under his parent's name, had connected to all eight cell towers. Dkt. 36-1 at 13-14. Of the cell phone numbers provided by the tower dumps, only Foster's had connected to all eight towers in the relevant time

frames. "[T]wo numbers [also] hit on six of the towers and an additional 10 numbers hit on five of the towers." *Id.* There was reason to believe that Foster used that particular cell phone because a 2018 police report filed by Foster had the cell phone number listed as contact information. *Id.* at 18-19. Further investigation revealed that Foster owned a Toyota RAV4. *Id.* at 18-19. More swastika stickers were placed at the Alaska Jewish Museum in September 2021. *Id.* at 41. There was also a public intersection vandalized with swastika graffiti. *Id.* at 40. Video recordings in both locations showed someone operating a one-wheeled scooter. *Id.* at 40-42. In September 2021 and October 2021, law enforcement monitored Foster's home, searched Foster's trash, and learned that Foster sold psilocybin mushrooms online after executing warrants on Foster's social media. *Id.* at 16-21, 26-33. Undercover law enforcement twice purchased psilocybin mushrooms from Foster in November 2021. *Id.* at 33-35. With that investigatory information gathered, three search warrants were then executed on Foster's person, vehicle, and home that same month. *Id.* at 38-39.

III. FOURTH AMENDMENT SEARCH

To this Court, the most vexing question presented is whether a Fourth Amendment search even occurred. *Carpenter*, 138 S. Ct. at 2220 n.4 (distinguishing the "threshold question [of] whether a search has occurred with the separate matter of whether the search was reasonable."); *see also Sanchez v. Los Angeles Dep't of Transportation*, 39 F.4th 548, 554 (9th Cir. 2022) ("The initial issue for decision is whether LADOT's collection of MDS location data is a search for Fourth Amendment purposes. Only if collection of the data is a search do we need to address the separate question of whether that search is

unreasonable."). The Supreme Court in *Carpenter*, 138 S. Ct. at 2220, declined to rule on whether a tower dump was a Fourth Amendment search. Although the Ninth Circuit has recently applied *Carpenter*, it has not ruled on Foster's particular question. *See e.g., Sanchez*, 39 F.4th at 556 (distinguishing between a cell phone and a rented electric scooter).

The Supreme Court has applied two Fourth Amendment frameworks to determine whether law enforcement investigation may be accurately characterized as a "search" within the meaning of the Fourth Amendment. The first stems from *Katz v. United States*, 389 U.S. 347, 361 (1967), where a concurrence established a two-pronged framework based on a reasonable expectation of privacy. *See also Florida v. Riley*, 488 U.S. 445 (1989) (ruling that a homeowner does not enjoy a reasonable expectation of privacy when law enforcement hovers over a house's curtilage with a helicopter); *see also California v. Greenwood*, 486 U.S. 35 (1988) (ruling that there is no reasonable expectation of privacy in trash left outside for disposal); *see also e.g., Riley v. California*, 573 U.S. 373, 392-401 (2014) (explaining the privacy issues presented by cell phone usage in modern times); *see also Carpenter*, 138 S. Ct. at 2215, 2220 (reasoning that there may be a reasonable expectation of privacy in a person's "physical location and movements."); *see also Sanchez*, 39 F.4th at 554-55.

As *Byrd v. United States*, 138 S. Ct. 1518, 1526 (2018) has reasoned, "property concepts are instructive in determining the presence or absence of the privacy interests protected[.]" (citing *Rakas v. Illinois*, 439 U.S. 128, 144 n.12 1978)). *Jones*, 565 U.S. at 406-07, and *Jardines*, 569 U.S. at 11, further reasoned that *Katz* supplemented rather than supplanted the property-based framework. Justice Kagan seemingly endorsed this line of

reasoning in her concurrence that analyzed the case "on privacy as well as property grounds." *Jardines*, 569 U.S. at 12.

This Court will employ both frameworks separately to ensure that Foster's constitutional rights are well-guarded.

Because the Fourth Amendment "protects people, not places," a search occurs "when an individual seeks to preserve something as private, and his expectation of privacy is one that society is prepared to recognize as reasonable[.]" *Carpenter*, 138 S. Ct. at 2213; *see also Sanchez*, 39 F.4th at 555 ("Thus the essential inquiry is whether collection of MDS location data violates a subjective expectation of privacy that society recognizes as reasonable.") (quoting *Kyllo*, 533 U.S. at 33) (internal quotations omitted). This privacy-based approach balances "Founding-era understandings" with modern technology that allows the government to "encroach upon areas normally guarded from inquisitive eyes." *Id.* at 2214. *Carpenter* acknowledged that cell site data which is "personal location information maintained by a third party [] does not fit neatly under existing precedents. Instead, requests for cell-site records lie at the intersection of two lines of cases, both of which inform our understanding of the privacy interests at stake." *Id.*; *Id.*

The first line of cases "addresses a person's expectation of privacy in his physical location and movements." *Id.* at 2215; *Id.* In *United States v. Knotts*, 460 U.S. 276, 281-82 (1983), the Supreme Court ruled that the government did not invade privacy interests when a GPS beeper was planted in a defendant's vehicle for tracking purposes. *Id.*; *Id.* "A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." *Id.*; *Id.* The Supreme Court in *Knots*,

however, cautioned that more invasive technology could trigger "different constitutional principles," such as "twenty-four hour surveillance." *Id.*; *Id.* Despite its property-based ruling, *Jones*, 565 U.S. at 404-05, five Justices raised privacy concerns from "surreptitiously activating a stolen vehicle detection system" in the defendant's vehicle or "conducting GPS tracking of his cell phone." *Id.*; *Id.* at 555-56. GPS monitoring on a "longer term" basis, Justice Alito concurred, "impinges on expectations of privacy." *Id.*; *Id.*

Critical here is *Carpenter*'s ruling that the government's acquisition of a defendant's cell-site location information ("CSLI") violated a reasonable expectation of privacy. *Sanchez*, 39 F.4th at 556 (citing *Carpenter*, 138 S. Ct. at 2217). *Carpenter* stressed that CSLI records "present even greater privacy concerns than the [*Jones*] GPS monitoring of a vehicle" because a cell phone has melded into a "feature of human anatomy." "Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user." *Id.* Moreover, the retrospective quality of CSLI allows the government to effortlessly "travel back in time to retrace a person's whereabouts, subject only to the retention policies of the wireless carriers." *Id.* Indeed, such inescapability results in "tireless and absolute surveillance for anyone with a cell phone." *Id.* The government in *Carpenter* therefore violated the defendant's reasonable expectation of privacy "in the whole of his physical movements." *Id. Carpenter*, however, made clear that its ruling was "a narrow one," in that "[w]e do not express a view on matters not before us: real-time CSLI or tower dumps." *Id.*

The second is a property-based framework, also referred to as a trespass framework. *See United States v. Jones*, 565 U.S. 400, 405 (2012) (ruling that a Fourth Amendment search occurred when law enforcement placed a GPS device on a private vehicle because it was a physical instruction, akin to a trespass-like act.); *see also Florida v. Jardines*, 569 U.S. 1, 133 (2013) (ruling that a K-9 sniffing a homeowner's front door was a physical intrusion); *see also Sanchez*, 39 F.4th at 554 ("For much of our Nation's history, the definition of a search under the Fourth Amendment was tied to common-law trespass, focusing on whether government actors had obtained information by physically intruding on a constitutionally protected area.") (internal quotations omitted).

To begin, *Riley*'s[5] observation that a cell phone is "an important feature of human anatomy" is undeniable. *Carpenter* strengthened this point when it reasoned that cell phones are intimately intertwined with the everyday life of the user and as a result, "a cell phone faithfully follows its owner beyond public thoroughfares … into other potentially revealing locales." *Carpenter*, 138 S. Ct. at 2218 (citing *Riley*, 573 U.S. at 395). Despite contracting with telephone companies, cell phone users expect, indeed, have a possessory interest that the contents of their phone be protected, including information-based property, against uninvited intrusions. *Riley*, 573 U.S. at 394-96 (citing Jones, 565 U.S. at 955). This reasoning tracks John Locke's concept of property that greatly influenced the Framers. Locke's broad view of property extended it beyond tangible things: "a person's rights, ideas, beliefs, and the creative products of her labor." Morgan Cloud, *Property is Privacy:*

[5] 573 U.S. at 385

Locke and Brandeis in the Twenty-First Century, 55 Am. Crim. L. Rev. 37 (2018); *see also* Locke, *The Second Treatise of Government* (C.B. Macpherson ed., 1980)) (explaining that governments were formed "for the mutual preservation of their lives, liberties, and estates, which I call by the general name, *property*."); *see also Carpenter*, 138 S. Ct. at 2239 (J., Thomas dissenting). The concept of property, in Locke's time, not only protected private papers themselves, but the contents of the papers; and it is along these lines, that Foster's cell site data should be protected too. Morgan Cloud, *supra* at 43. Locke's theory of property elevated the idea of private ownership from the practical to the political in 18th century America, which led James Madison to expound on the concept of property. *Id.* at 44. Madison's writings, stressed that aside from tangible things, "[t]he praise of affording a just securing to property, should be sparingly bestowed on a government which, however scrupulously guarding the possessions of individuals, does not protect them in the enjoyment and communication of their opinions, in which they have an equal, and in the estimation of some, a more valuable property." *Id.* at 49-50; *see also* James Madison, *Property*, *The Writings of James Madison 101* (Gaillard Hunt ed., 1906) (reasoning "that a man has a property in his opinions and the free communication of them … [that the] safety and liberty of his person is property very dear to him.").

In calling for a return to the traditional approach of Fourth Amendment protections of (1) person, (2) home, (3) papers, or (4) effects, Justice Gorsuch emphasized that these four objects "protect privacy in particular places and things … and against particular threats. *Carpenter*, 138 S. Ct. at 2264. Justice Gorsuch further explained that referring to Framer era values would ensure protecting both "the specific rights known the founding"

and "their modern analogues too." Under this guidance, this Court views similarities between private papers that are "locked safely in a desk drawer or destroyed," and cell phones that exclude the public from the cell phone's contents with password-protected mechanisms. People use passwords because cell phones store a significant amount of data that can be utilized to reconstruct an individual's private life and movements. These privacy interests have a heightened importance, when as here, the government had an intent to prosecute when it was *searching* for one individual that vandalized eight different locations. This Court agrees with the government that cell-site tracking data "can shed a great deal of light on the location of that person. In addition to establishing what locations a particular person might have gone to, providers can also help identify which people might have been in a particular location[.]" Dkt. 42 at 3-4; Dkt. 36-2 at 5, 9-11. To this Court, the government's acquisition of Foster's cell-site tracking data had all the hallmarks of a Fourth Amendment search.

In an effort to proceed with caution, this Court first turns to 18th century common law that tracks a broad conception of property rights. *Carpenter*, 138 S. Ct. at 2264 (J., Gorsuch dissenting). The first case was brought by John Wilkes, an English radical and author of several tracts that were critical of government policies. *Id.* (citing *Wilkes v. Wood*, 19 How St. Tr. 1153 (K.B. 1763)); *see also* Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 Ind. L.J. 979, 1006-07 (2011). Regarding the seized private papers, *Wilkes* reasoned that "for other offences, acknowledgement might make amends; but for the promulgation of our most private concerns, affairs of the most secret personal nature, not reparation whatsoever could be made." Laura K. Donohue,

The Original Fourth Amendment, 83 U. Chi. L. Rev. 1181, 1203-04 (2016). *Wilkes* gave rise to *Entick* which has been "described as a monument of English freedom[,] undoubtedly familiar to every American statesman at the time the Constitution was adopted, and considered to be the true and ultimate expression of constitutional law with regard to search and seizure." *Jones*, 565 U.S. at 405 (internal quotations omitted) (citing *Entick v. Carrington*, 95 Eng. Rep. 807 (C.P. 1765)). Despite *Entick*'s narrow ruling regarding general warrants, the seizure of private papers was at the forefront of the opinion: "Papers are the owner's goods and chattels: they are his dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection; and though the eye cannot by the laws of England be guilty of a trespass, yet where private papers are removed and carried away, the secret nature of those goods will be an aggravation of the trespass … subversive of all the comforts of society." *Entick v. Carrington*, 95 Eng. Rep. 807 (C.P. 1765)). The third case was known as the *Writs of Assistance Case*, where "patriot James Otis" condemned the use of general warrants because it infringed on an individual's freedom to be secure in one's household. *See Carpenter*, 138 S. Ct. at 2213, 2240 (J., Thomas dissenting); *see also Riley*, 573 U.S. at 403.

The Supreme Court has applied "these ancient principles," to modern technology as well. *Kyllo v. United States*, 533 U.S. 27, 34 (2001) ruled that technology that allows the government to look inside "the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area constitutes a search—at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when

the Fourth Amendment was adopted." (citation cleaned up); *see also* Morgan Cloud, *supra* at 69 (explaining that *Kyllo* "melded property theory and nontrespassory technological surveillance—the *functional equivalent of a trespass*) (emphasis in original). Somewhat resurrecting the common-law trespass framework, *Jones*, 565 U.S. at 404, ruled that the government's use of a GPS location device placed on a defendant's vehicle was a Fourth Amendment search because the movements of the defendant's vehicle were tracked. *Jones* strengthened a property-based approach to the Fourth Amendment all the while balancing the *Katz* privacy framework. *Id.* at 405-06, 411; *see also* Morgan Cloud, *supra* at 71 ("What connects the ideas expressed by Locke, Camden, Madison, Brandeis, and Scalia, and those expressed in judicial opinions like *Entick* and *Boyd*, is not the legal categories--privacy or property--to which their ideas frequently are assigned. They are connected instead by shared fundamental values that survive across centuries and continents.").

Justice Gorsuch has also pointed out that *Ex Parte Jackson*, 96 U.S. 727, 733 (1878) already set "the constitutional floor" as to the private contents of "papers." *Ex Parte Jackson* ruled that private, sealed letters sent via government mail, were protected by the Fourth Amendment, much like "when papers are subjected to search in one's own household." The Fourth Amendment "extends to their papers, thus closed against inspection, wherever they may be." *Carpenter*, 138 S. Ct. at 2269 (quoting *Ex Parte Jackson*, 96 U.S. at 733); *see also Silverthorne Lumber Co. v. United States*, 251 U.S. 385, 391 (1920) (reasoning that the Fourth Amendment protected the "physical possession" of papers and against "any advantages the government may enjoy through its illegal acts."). Other cases, despite privacy influences from *Katz*, exhibit some acknowledgement of a

property-based framework. *See Silverman v. United States*, 365 U.S. 505, 506-07 (1961) (ruling that a "spike mike" was a physical intrusion of the household); *Wong Sun v. United States*, 371 U.S. 471, 485 (1963) (reasoning that "the Fourth Amendment may protect against the overhearing of verbal statements as well as against the more traditional seizure of paper and effects.") (internal quotations omitted); *see also Berger v. New York*, 388 U.S. 41, 51 (1967) (attempting to reconcile privacy and the concept of property); *see also Carpenter*, 138 S. Ct. at 2236-37 (J., Alito dissenting).

In tandem with the views in *Riley* and *Carpenter* that cell phones and the data they contain are property, Justice Gorsuch further reasoned that "countless Internet companies maintain records about us, and increasingly, *for* us." *Carpenter*, 138 S. Ct. at 2262. In other words, a person's possessory interest in their information-based property is not vitiated when "you entrust your data—in some cases, your modern-day papers and effects—to a third party." *Id.* at 2268. The law of bailment is instructive in this regard. A bailor who entrusts property to a bailee, including information-based property, does not lose the property or rights to the property; it remains the bailor's. *Id.* (citing *Ex Parte Jackson*, 96 U.S. at 733); *see also Jones*, 565 U.S. at 404 n.2 (explaining that the defendant "had at least the property rights of a bailee" despite not owning the vehicle in question), 425 (J., Alito concurrence) (reasoning that a "bailee may sue for a trespass to chattel only if the injury occurs during the term of the bailment.) (citing 8A Am. Jur .2d, Bailment § 166, pp. 685-86 (2009)). This is particularly important when one accounts for the *ineluctable necessity* of owning a cell phone in modern society, which may be, as Justice Gorsuch reasons, involuntary bailment. *Carpenter*, 138 S. Ct. at 2270 (J., Gorsuch dissenting).

Federal courts can also "look to positive law rather than intuition for guidance on social norms." *Id.* at 2265. "[P]ositive law or analogies to items protected by the enacted Constitution" can balance "Fourth Amendment protections for your papers and effect [that] do not automatically disappear just because you share them with third parties." *Id.* at 2268. Aside from the aforementioned 18th century common law and recent Supreme Court jurisprudence, federal laws and state laws can serve as positive law. *Id.* at 2270. On this point, the government's points on positive law are well taken. Dkt. 42 at 9-10. It is not entirely clear whether the federal legislation cited by Foster can serve as positive law, but applying the principles in Justice Gorsuch's dissent, this Court concludes that the cited federal legislation establishes *some* possessory interests in cell site tracking data.

This Court first turns to 47 U.S.C. § 222, "Privacy of customer information." Section 222(a) states that telephone companies have a "duty to protect the confidentiality of *proprietary* information of, and relating to …. customers[.]" (emphasis added). Customer proprietary information is defined as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship." 47 U.S.C. § 222(h)(1)(A). Telephone companies are mandated to ensure that a customer's proprietary information is only used to provide "any telecommunications service." A telephone company, however, can "disclose" or permit access to individually identifiable customer proprietary network information" if the customer allows it or "as required by law." § 222(c)(1)-(2). If the law does not require

disclosure, a telephone company needs a customer's express approval to disclose or use "call location information concerning the user of a commercial mobile service," or when needed to notify customers of an automatic crash. § 222(f)(1)-(2).

A careful reading of this statute indicates that § 222 restricts a telephone company's use of a customer's proprietary information and also allows a customer to move for damages in the event that a telephone company violates § 222. *See Carpenter*, 138 S. Ct. at 2272. Section 222 also vests in the customer some discretion as to the telephone company's use of proprietary information. The flaw in Foster's argument that § 222 by itself creates a property right in the customer's proprietary information is the "[e]xcept as required by law" language of § 222. This language is neither vague nor subject to different interpretations. Justice Gorsuch, however, stressed that Fourth Amendment protections do not require complete ownership or exclusive control of property. *Id.* An individual, for example, has a zealously guarded possessory interest in their house, even when the bank possesses the legal title, when the house is instead rented to tenants, or when it is occupied without any monetary payment. *Id.* (citing *Carter*, 525 U.S. at 95-96). Justice Gorsuch also notes that "positive law cannot be used to defeat" Fourth Amendment protections. *Id.* at 2270 (citing *Ex Parte Jackson*, 96 U.S. at 733). As this Court has mentioned, the concept of property that stems from 18th century common law and Justice Gorsuch's dissent, can help address the nuances of modern technology. Positive law, much like *Ex Parte Jackson*'s reasoning, can provide a floor to Fourth Amendment protections because the cornerstone of the Fourth Amendment, after all, is reasonableness. If a cell phone provider disclosed a customer's proprietary information "as required by law," or specifically

through a 18 U.S.C. § 2703(c)(1)(A) warrant, that could very well rebut any arguments regarding reasonableness. Perhaps equally consistent with Justice Gorsuch's view is to simply disrobe the government of their "official authority" and ask if "the government [has] done something that would be tortious, criminal, or otherwise a violation of some legal duty? Fourth Amendment protection, in other words is warranted when government officials either violated generally applicable law or avail themselves of a governmental exemption from it." William Baude, James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 Harv. L. Rev. 1821, 1825-26 (2016). Through that view, it might be easier to answer in the affirmative, that a search did occur in Foster's case.

In the end, Justice Gorsuch nonetheless expressed a willingness to conclude that a "person's cell-site data could qualify as *his* papers or effects under existing law." Having carefully reviewed the relevant frameworks, case law, arguments of counsel, and all of the facts and circumstances of Foster's case, this Court agrees. Foster's cell site tower data are his "papers" within the meaning of the Fourth Amendment. The government therefore conducted a Fourth Amendment search when it acquired Foster's cell site tower data.

IV. JUNE 2021 WARRANT

The Fourth Amendment provides that a valid warrant must describe "the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV. "Specificity has two aspects: particularity and breadth. Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by probable cause on which the warrant is based." *United States v. Banks*, 556 F.3d 967, 972-73 (9th Cir. 2009) (citing *United States v. Hill*, 459 F.3d 966, 973

(2006)). The purpose behind the specificity requirement is to protect against arbitrary government intrusions, and to "safeguard the privacy and security of individuals" from sweeping overbroad warrants. *Carpenter*, 138 S. Ct. at 2213 (quoting *Camara v. Municipal Court of City and County of San Francisco*, 387 U.S. 523, 528 (1967)); *see also United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986) (reasoning that a warrant's description "must be specific enough to enable the person conducting the search reasonable to identify the things authorized to be seized."). It is important to remember that probable cause is a lower standard than preponderance of the evidence. *Illinois v. Gates*, 465 U.S. 213, 235 (1983) (explaining that "[f]inely-tuned standards such as proof beyond a reasonable doubt or by a preponderance of the evidence, useful in formal trials, have no place" in a probable cause determination and is instead a practical inquiry based on the totality of the circumstances."). The totality of the circumstances test is a "practical, nontechnical conception." *Id.* at 231.

This Court first declines Foster's invitation to impose "strict minimization requirements" or to prescribe a certain standard for obtaining cell-site tracking data. Dkt. 36 at 21-25. It is sufficient here that the government established both the statutory standard in § 2703(d) and the probable cause standard for a search warrant.

Foster argues that the government "should be required to aver in its warrant application that is has exhausted less invasive means of identifying the suspect." Dkt 36 at 22. Foster argues by analogy that since such a requirement exists in the case of wiretap warrants, it should similarly apply here. *Id*. This argument is not persuasive. As an initial matter, the requirement that wiretap warrants represent that less intrusive means have been

exhausted is a function of the wiretap statute.[6] Should Congress fashion such a requirement for CSLI, that is their prerogative, but this Court will not invent such a requirement because it may exist for other classes of digital evidence. Further, the comparison between wiretap warrants and the warrant in this case is inapposite. Wiretaps seek substantive communications. Here, the warrant sought, and obtained, only information regarding which cell numbers had connected to certain cell towers, at certain times. While both constitute Fourth Amendment searches, a search implicating substantive communications (wiretaps) is far more intrusive, as compared with searches which do not reveal an individual's thoughts or communications. The reasonableness of the two classes of searches therefore differs dramatically.

Foster argues for a number of procedural protections regarding the data of individuals not suspected of a crime. Dkt 36, at 24-25. It is unclear how Foster has standing to object to the handling of data belonging to other people. *See Rakas v. Illinois*, 439 U.S. 128, 140 (1978) (""Fourth Amendment rights are personal rights, which like some other constitutional rights, may not be vicariously asserted."); *see also Carpenter*, 128 S. Ct. at 2226-27 (J., Kennedy dissenting), 2237 (J., Thomas dissenting), 2257 (J., Alito dissenting).

Foster further argues that "warrants for tower dumps should be required to mitigate the intrusion into the private lives of proximate individuals." *Id*. at 23. To the extent that Foster argues this point as a general principle, this Court agrees. To the extent that Foster presumes to have standing to vindicate the rights of other individuals, he is mistaken. See

[6] 18 USC § 2518(1)(c)

Id. To the extent that the argument is that the warrants in this case did not mitigate the intrusion into the lives of individuals, that argument is counter-factual and is not well taken. Here, the location of the particular towers was limited to those towers close to known areas of vandalism. *See* e.g., Dkt 36-2. Data from those towers was constrained to narrow timeframes when the vandalism was known to have occurred. *Id*. The data obtained by law enforcement was limited to cell numbers, with no subscriber information. Of the cell numbers obtained, only one had connected to all towers in the relevant time frame. It was this one number that led law enforcement to Foster. In other words, the warrant in this case was narrowly tailored, circumspect, sought no substantive communications, and was therefore a reasonable search under the Fourth Amendment.

Many of Foster's arguments seem to overlook the fact that law enforcement applied for and was granted a warrant which was supported by probable cause. SA Oberlander described in particular detail that Foster wore the same clothing at all recorded locations: (1) sandals, (2) dark-colored socks, (3) dark colored pants, (4) dark colored hooded sweatshirt, (5) long-sleeved shirt, and (6) dark balaclava type head and face covering. Critical here is that the affidavit also included photographs that confirmed the clothing description and Foster's modes of transportation. This is sufficient for probable cause purposes because the particular details allowed the issuing judicial officer to reasonably conclude that it was the *same* person at all of the vandalized locations. The *modus operandi* was consistent from location to location as well: the suspect was seen on surveillance video operating a Toyota Rav4, a one-wheel scooter, and making obscene gestures. Aside from describing the Nazi-themed vandalism, the affidavit described the targeted locations in

particular detail, and the fear it caused in the targeted communities. 18 U.S.C. § 245. Taking that information together, the affidavit established that Foster intended to intimidate or threaten members of the Jewish community, LGTBQ+ community, and persons associated with Planned Parenthood. Perhaps most importantly, the affidavit stated (and provided photographs) of Foster using "what appears to be a cell phone to take photographs and or text." This Court credits SA Oberlander's statement that, in his training and experience, "it is common for criminals to use cellular telephones while engaged in criminal behavior, even if that usage is not directly related to the crimes committed" which, in turn, established "probable cause to believe that the cell towers servicing the locations described … will contain records of cellular activity from the phone used." In that regard, *Carpenter* and *Riley*'s recognitions of the ubiquitous use of cell phones strengthens the credibility of SA Oberlander's statements. This Court therefore concludes that SA Oberlander established probable cause to believe that 18 U.S.C. §§ 245 (Federally Protected Activities), 247 (Damage to Religious Property; Obstruction of Persons in the Free Exercise of Religious Beliefs, and 248 (Freedom of access to Clinic Entrances) had been violated, and that a search for the contemplated information would lead to evidence of the perpetrator thereof.

Even if the search warrants were deemed invalid, *Leon's* good-faith exception would nonetheless apply. In *United States v. Leon*, 468 U.S. 897, 919-21 (1984), "the exclusionary rule should not be applied to exclude evidence seized pursuant to a defective search warrant if the officers conducting the search acted in 'objectively reasonable reliance' on the warrant and the warrant was issued by a detached and neutral magistrate[.]"

There is no suggestion that SA Oberlander acted in bad faith when he applied for the search warrant. Under these circumstances, there is nothing in the record to suggest that the search warrant affidavits objectively lack probable cause, nor is it obvious that the search warrants themselves are unconstitutional.

V. CONCLUSION

For the reasons set forth above, Foster's Motion to Suppress [Dkt. 36] should be **DENIED**. 28 U.S.C. § 636(b)(1)(B).

DATED this 17th day of November, 2022, at Anchorage, Alaska.

s/ Matthew M. Scoble
CHIEF U.S. MAGISTRATE JUDGE

Pursuant to D. Alaska Loc. Mag. R. 6(a), a party seeking to object to this proposed finding and recommendation shall file written objections with the Clerk of Court no later than the CLOSE OF BUSINESS on November 28, 2022. Failure to object to a magistrate judge's findings of fact may be treated as a procedural default and waiver of the right to contest those findings on appeal. Miranda v. Anchondo, et al., 684 F.3d 844 (9th Cir. 2012). The Ninth Circuit concludes that a district court is not required to consider evidence introduced for the first time in a party's objection to a magistrate judge's recommendation. United States v. Howell, 231 F.3d 615 (9th Cir. 2000). Objections and responses shall not exceed five (5) pages in length, and shall not merely reargue positions presented in motion papers. Rather, objections and responses shall specifically designate the findings or recommendations objected to, the basis of the objection, and the points and authorities in support. Response(s) to the objections shall be filed on or before the CLOSE OF BUSINESS on December 5, 2022. The parties shall otherwise comply with provisions of D. Alaska Loc. Mag. R. 6(a). Reports and recommendations are not appealable orders. Any notice of appeal pursuant to Fed. R. App. P. 4(a)(1) should not be filed until entry of the District Court's judgment. See Hilliard v. Kincheloe, 796 F.2d 308 (9th Cir. 1986).